

(11)Publication number : 2000-076136  
(43)Date of publication of application : 14.03.2000

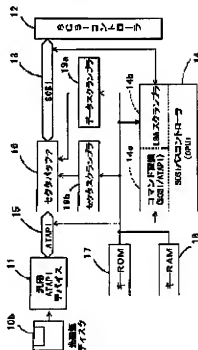
G06F 12/14  
G11B 20/10

(71)Applicant : MELCO INC

(72)Inventor : SAITO SHINSUKE  
HIRUMA MASAHIRO

(57) Abstract:

**SOLUTION:** In recording the data to a magneto-optical disk 10b, the data themselves are ciphered by a data scrambler 19a and a sector scrambler 19b and they are recorded while scrambling the LBA of a sector by the LBA scrambler logic 14b of an SCSI bus controller 14. At the read of the recorded data, they are read while restoring the LBA by the LBA scrambler logic 14b of the SCSI bus controller 14 and the data themselves are deciphered and outputted by the data scrambler 19a and the sector scrambler 19b.



(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 1 1 B 20/10		G 1 1 B 20/10	H 5 D 0 4 4

審査請求 未請求 請求項の数10 O L (全 12 頁)

(21) 出願番号 特願平10-241982

(22) 出願日 平成10年8月27日 (1998.8.27)

(71) 出願人 390040187

株式会社メルコ

愛知県名古屋市中区大須4丁目11番50号

(72) 発明者 斎藤 伸介

名古屋市南区桑田本通四丁目15番 株式会社

社メルコハイテクセンター内

(72) 発明者 蛭間 正浩

名古屋市南区桑田本通四丁目15番 株式会社

社メルコハイテクセンター内

(74) 代理人 100096703

弁理士 横井 俊之

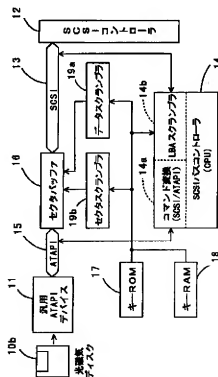
最終頁に続く

## (54) 【発明の名称】 記録再生装置

## (57) 【要約】

【課題】 データ自体を暗号化して記録媒体に記録した場合、暗号化が解除されてデータが盗用される危険があった。

【解決手段】 光磁気ディスク10bに対してデータを記録するにあたり、データスクランブラ19aおよびセクタスクランブラ19bによってデータ自体を暗号化するとともに、SCSIバスコントローラ14のLBAスクランブラロジック14bによってセクタのLBAをスクランブルしつつ記録し、記録したデータを読み出すにあたっては、SCSIバスコントローラ14のLBAスクランブラロジック14bによってLBAを復元しつつ読み出すとともに、データスクランブラ19aおよびセクタスクランブラ19bによってデータ自体を復号化して出力するようにした。



## 【特許請求の範囲】

【請求項 1】 所定の鍵情報を記憶する鍵情報記憶手段と、

入力データをセクタ単位に所定の記録媒体に記録するにあたり、各セクタの同記録媒体上における論理アドレスを上記鍵情報に基づいてスクランブルしつつ記録するスクランブル記録手段と、

上記記録媒体に記録されたデータをセクタ単位に読み出すにあたり、スクランブルされた各セクタの論理アドレスを上記鍵情報に基づいて復元しつつ読み出すスクランブル解除読出手段とを具備することを特徴とする記録再生装置。

【請求項 2】 上記請求項 1 に記載の記録再生装置において、上記鍵情報記憶手段は、上記鍵情報を変更可能に記憶することを特徴とする記録再生装置。

【請求項 3】 上記請求項 2 に記載の記録再生装置において、上記鍵情報記憶手段は、上記鍵情報が記録された所定の鍵情報 ROM を脱着可能である、装着された鍵情報 ROM から同鍵情報を取得して記憶することを特徴とする記録再生装置。

【請求項 4】 上記請求項 2 に記載の記録再生装置において、上記鍵情報記憶手段は、上記記録媒体に記録された鍵情報を取得して記憶することを特徴とする記録再生装置。

【請求項 5】 上記請求項 1～請求項 4 のいずれかに記載の記録再生装置において、上記記録媒体は当該記録再生装置に対して脱着可能であることを特徴とする記録再生装置。

【請求項 6】 上記請求項 1～請求項 5 のいずれかに記載の記録再生装置において、上記スクランブル記録手段は、上記鍵情報に基づいて上記入力データをセクタ毎に暗号化しつつ、上記論理アドレスをスクランブルして上記記録媒体に記録し、

上記スクランブル解除読出手段は、上記論理アドレスのスクランブルを復元しつつセクタ毎に読み出し、読み出したセクタ毎に上記鍵情報に基づいて復号化して出力することを特徴とする記録再生装置。

【請求項 7】 上記請求項 6 に記載の記録再生装置において、上記スクランブル記録手段は、上記鍵情報に基づいて上記セクタを構成する各ワード毎に暗号化し、上記スクランブル解除読出手段は、読み出したセクタ毎に上記鍵情報に基づいて各ワードを復号化して出力することを特徴とする記録再生装置。

【請求項 8】 上記請求項 6 または請求項 7 に記載の記録再生装置において、上記スクランブル記録手段は、上記鍵情報に基づいて上記セクタを構成する各ワードを同一セクタ内でスクランブルし、

上記スクランブル解除読出手段は、読み出したセクタ毎に上記鍵情報に基づいてスクランブルされた各ワードを復元して出力することを特徴とする記録再生装置。

【請求項 9】 上記請求項 1～請求項 8 のいずれかに記載の記録再生装置において、上記スクランブル記録手段およびスクランブル解除読出手段は、ホスト装置との間で入力データを転送するための第一のバスと、上記記録媒体との間で入力データを転送するための第二のバスと、

上記第一および第二のバス間に介在するとともに、それぞれのバスから転送されるデータをセクタ単位で格納可能なセクタバッファと、

上記記録媒体に対してそれぞれデータ記録およびデータ読出を行うにあたり、一方のバスから転送されるデータを上記セクタバッファにセクタ単位で格納させつつ上記第一のバスと第二のバスとの間でバス変換して他方のバスにデータを出力するバス変換手段とを具備することを特徴とする記録再生装置。

【請求項 10】 上記請求項 9 に記載の記録再生装置において、上記第一および第二のバスは、一方が SCSI であるとともに他方が ATAPI であることを特徴とする記録再生装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、記録再生装置に関し、特に、記録媒体に記録されたデータの盗用などを防止することが可能な記録再生装置に関する。

## 【0002】

【従来の技術】 従来、この種の記録再生装置の一例として、特開昭 63-219044 号公報や特開平 9-73414 号公報などに開示されたものが知られている。前者に開示されたものにおいては、所定の鍵情報に基づいてデータを暗号化して記録媒体に記録するようになっており、このように記録されたデータを再生する場合には、同記録媒体から読み出したデータを上記鍵情報に基づいて復号化して出力する。

【0003】 一方、後者に開示されたものにおいては、光ディスクなどの記録媒体にデータを記録する場合に、入力デジタルデータをセクタ化するセクタ工程、その後ヘッダを付加するヘッダ付加工程、その後誤り訂正符号を付加する誤り訂正符号化工程、そして所定の変調方式で変調する変調工程、その後同期パターンを付加する同期付加工程のいずれか一つの工程に人力に対して暗号化処理を施すようになっている。

## 【0004】

【発明が解決しようとする課題】 上述した従来の記録再生装置においては、次のような課題があった。前者においては、データが暗号化されているので確かに記録媒体上のデータが盗用される可能性は低いと言える。しかし、記録媒体からデータを読み出すことは可能であるため、暗号が解読される危険性があることは否定できない。一方、後者においては、各工程で適宜暗号化処理を

施せば、記録媒体上のデータが盗用される可能性はかなり低いと言える。しかし、TOC情報などが含まれるリードイン領域は各光ディスクで固定されているため、かかるリードイン領域から情報を取得して暗号が解読される危険性があることは否定できない。

【0005】本発明は、上記課題にかんがみてなされたもので、より確実に記録媒体上のデータの盗用などを防止することが可能な記録再生装置の提供を目的とする。

【0006】

【課題を解決するための手段】上記目的を達成するため、請求項1にかかる発明は、所定の鍵情報を記憶する鍵情報記憶手段と、入力データをセクタ単位に所定の記録媒体に記録するにあたり、各セクタの同記録媒体上における論理アドレスを上記鍵情報に基づいてスクランブルしつつ記録するスクランブル記録手段と、上記記録媒体に記録されたデータをセクタ単位に読み出すにあたり、スクランブルされた各セクタの論理アドレスを上記鍵情報に基づいて復元しつつ読み出すスクランブル解除読み手段とを備えた構成とである。

【0007】上記のように構成した請求項1にかかる発明においては、記録媒体に対するデータの記録および読出においてはセクタ単位に行われることを前提としており、データ記録時においてスクランブル記録手段は、各セクタの記録媒体上における論理アドレスを鍵情報記憶手段に記憶された鍵情報に基づいてスクランブルしつつ記録する。一方、データ読出時においてスクランブル解除読み手段は、スクランブルされた各セクタの論理アドレスを上記鍵情報に基づいて復元しつつ読み出す。

【0008】むしろ、ここにおけるスクランブルとは、本来、書き込むべきセクタの論理アドレスを同一の記録媒体内でランダムに入れ換えることを意味している。例えば、複数のセクタに跨るようなデータが記録される場合、記録媒体上で複数の連続するセクタが空いていたとしても同連続するセクタにデータが書き込まれることはなく、実際にデータが記録されるセクタはランダム化される。従来、FAT情報等が記録されるセクタは固定されているが、むしろ、本発明においてはかかるセクタの論理アドレスも当然にスクランブルの対象となる。従って、仮に記録媒体のみを持ち出してデータを盗用しようとしても、別の再生装置ではFAT情報等を読み取ることができず、記録媒体上におけるセクタ間のデータ関連性も判明しないため、データが盗用される可能性は極めて低いと言える。

【0009】上記のようなスクランブル処理に利用する鍵情報は、各装置で固定の情報として記憶されていてもよいが、別の好適な一例として、請求項2にかかる発明は、請求項1に記載の記録再生装置において、上記鍵情報記憶手段は、上記鍵情報を変更可能に記憶する構成とである。上記のように構成した請求項2にかかる発明においては、鍵情報記憶手段に記憶された鍵情報を変更

することが可能であり、適宜、利用者等が鍵情報を設定する。

【0010】具体的には、利用者に所望の値を入力させ、その入力値に基づいて鍵情報を設定するなどの構成とすることも可能であるが、別の一例として請求項3にかかる発明は、請求項2に記載の記録再生装置において、上記鍵情報記憶手段は、上記鍵情報が記録された所定の鍵情報ROMを脱着可能であり、装着された鍵情報ROMから同鍵情報を取得して記憶する構成としてある。

【0011】上記のように構成した請求項3にかかる発明においては、鍵情報を鍵情報記憶手段に記憶させる場合には所定の鍵情報ROMを装着する。すると、鍵情報記憶手段によって同鍵情報ROMに記録された鍵情報が読み取られて記憶される。例えば、利用者に提供するにあたり、記録再生装置本体と複数の鍵情報ROMとを併せて利用者に提供し、利用者によって所望の鍵情報ROMを選択させる構成としてもよい。

【0012】むしろ、鍵情報を記録する記録媒体としては必ずしも専用の鍵情報ROMに限られることはなく、別の一例として請求項4にかかる発明は、請求項2に記載の記録再生装置において、上記鍵情報記憶手段は、上記記録媒体に記録された鍵情報を取得して記憶する構成とである。すなわち、本来、データが記録される記録媒体に鍵情報が記録されており、鍵情報記憶手段は同記録媒体から鍵情報を取得して記憶する。むしろ、ここにおける鍵情報は、記録媒体上にデータとして記録されているものであってもよいし、各記録媒体に固有のシリアル番号などを利用するものであってもよい。

【0013】ところで、近年においては記録媒体自体が小型化、大容量化され、信頼性も高いことから、かかる記録媒体上のデータ盗用を防止する必要性が高まりつつある。そこで、本発明がより有効に機能する構成の一例として、請求項5にかかる発明は、請求項1～請求項4のいずれかに記載の記録再生装置において、上記記録媒体は当該記録再生装置に対して脱着可能な構成としてある。

【0014】上記のように構成した請求項5にかかる発明においては、上記のようにしてデータが記録された記録媒体を取り外して持ち運ぶことが可能であり、仮に記録媒体自体が盗難された場合であっても記録されたデータを読み取ることは極めて困難である。むしろ、かかる記憶媒体としては多種多様であって特に限定されることはなく、例えば、フロッピーディスク、光磁気ディスクやDVD-RAMなど各種形態のものを適用可能である。

【0015】スクランブル記録手段は、記録媒体上におけるセクタの論理アドレスをスクランブルしつつデータを記録するため、記録媒体上に記録されたデータの盗用などを防止することできることになるが、かかるデータ

10

20

30

40

50

の盗用などをより効果的に防止しうる構成の一例として、請求項 6 にかかる発明は、請求項 1～請求項 5 のいずれかに記載の記録再生装置において、上記スクランブル記録手段は、上記鍵情報に基づいて上記入力データをセクタ毎に暗号化し、上記論理アドレスをスクランブルして上記記録媒体に記録し、上記スクランブル解除読出手段は、上記論理アドレスのスクランブルを復元しつつセクタ毎に読み出し、読み出したセクタ毎に上記鍵情報に基づいて復号化して出力する構成としてある。

【0016】上記のように構成した請求項 6 にかかる発明においては、スクランブル記録手段は、上記鍵情報に基づいてセクタ毎に入力データを暗号化するとともに、上記のように記録媒体上における各セクタの論理アドレスをスクランブルして記録する。従って、このように記録されたデータを読み出す場合には、スクランブル解除読出手段が読出対象となるセクタの論理アドレスを復元しつつセクタ毎に読み出し、読み出したセクタ毎に上記の鍵情報に基づいて復号化して出力する。すなわち、上記のような論理アドレスのスクランブルと、セクタ毎のデータの暗号化とを併用することによってデータの盗用

10

20

などをより効果的に防止する。  
【0017】これにおける暗号化とは、実際のデータを暗号化してデータの読出を困難にする手法を広く含むものであり、その一例として、請求項 7 にかかる発明は、請求項 6 に記載の記録再生装置において、上記スクランブル記録手段は、上記鍵情報に基づいて上記セクタを構成する各ワード毎に暗号化し、上記スクランブル解除読出手段は、読み出したセクタ毎に上記鍵情報に基づいて各ワードを復号化して出力する構成としてある。

【0018】上記のように構成した請求項 7 にかかる発明においては、スクランブル記録手段は、セクタを構成する各ワードを鍵情報に基づいて暗号化し、さらに上記の論理アドレスのスクランブルを行って記録媒体に記録する。そして、実際にデータを読み出すにはスクランブル解除読出手段が論理アドレスを復元しつつセクタ単位に読み出し、各セクタにおける各ワードを鍵情報に基づいて復号化して出力する。

【0019】また、このようにワード単位に暗号化が施されているか否かにかかわらず、別の暗号化の一例として、請求項 8 にかかる発明は、請求項 6 または請求項 7 に記載の記録再生装置において、上記スクランブル記録手段は、上記鍵情報に基づいて上記セクタを構成する各ワードを同一セクタ内でスクランブルし、上記スクランブル解除読出手段は、読み出したセクタ毎に上記鍵情報に基づいてスクランブルされた各ワードを復元して出力する構成としてある。

【0020】上記のように構成した請求項 7 にかかる発明においては、スクランブル記録手段は、セクタを構成する各ワードを鍵情報に基づいて同一セクタ内でスクランブルし、さらに上記の論理アドレスのスクランブルを

行って記録媒体に記録する。そして、実際にデータを読み出すにはスクランブル解除読出手段が論理アドレスを復元しつつセクタ単位に読み出し、各セクタにおいて鍵情報に基づいてスクランブルされた各ワードを復元して出力する。むしろ、ここにおいて各ワードを同一セクタ内でスクランブルすることは、同一セクタ内で各ワードをランダムに入れ換えることを意味する。

【0021】本発明にかかる記録再生装置は、P C などのホスト装置に接続されて使用されることを前提としているが、いかなるインターフェイスを採用するかについては全くの任意である。また、近年においては各種仕様のインターフェイスが開発され、現実利用されていることにかんがみ、請求項 9 にかかる発明は、請求項 1～請求項 8 のいずれかに記載の記録再生装置において、上記スクランブル記録手段およびスクランブル解除読出手段は、ホスト装置との間で入出力データを転送するための第一のバスと、上記記録媒体との間で入出力データを転送するための第二のバスと、上記第一および第二のバス間に介在するとともに、それぞれのバスから転送されるデータをセクタ単位で格納可能なセクタバッファと、上記記録媒体に対してそれぞれデータ記録およびデータ読出を行うにあたり、一方のバスから転送されるデータを上記セクタバッファにセクタ単位で格納させて上記第一のバスと第二のバスとの間でバス変換して他方のバスにデータを読み出すバス変換手段とを備えた構成としてある。

【0022】上記のように構成した請求項 9 にかかる発明においては、スクランブル記録手段が記録媒体にデータを記録する場合、バス変換手段は第一のバスから転送されるデータをセクタ単位にセクタバッファに格納させつつ、同第一のバスと第二のバスとの間でバス変換して第二のバスにデータを転送して記録媒体に記録する。他方、スクランブル解除読出手段が記録媒体からデータを読み出す場合、バス変換手段は第二のバスから転送されるデータをセクタ単位にセクタバッファに格納させつつ、同第二のバスと第一のバスとの間でバス変換して第一のバスにデータを転送して出力する。

【0023】また、かかる場合のより具体的な構成の一例として、請求項 10 にかかる発明は、請求項 9 に記載の記録再生装置において、上記第一および第二のバスは、一方が S C S I であるとともに他方が A T A P I で構成してある。すなわち、主に P C などの外付装置のインターフェイスとして利用される S C S I と、主に内蔵装置のインターフェイスとして利用される A T A P I との間で適宜バス変換しつつデータ記録およびデータ読出を行う。

【0024】

【発明の効果】以上説明したように本発明は、記録媒体に対するデータを記録するにあたり、各セクタの記録媒

50

体上における論理アドレスを鍵情報に基づいてスクランブルしつつ記録し、読み出しにはスクランブルされた各セクタの論理アドレスを上記鍵情報に基づいて復元しつつ読み出すようにしたため、記録媒体上のセクタ間のデータの関連性がランダムとなって一般の再生装置によっては記録媒体上のFAT情報等も読み取ることができなくなり、より確実に記録媒体上のデータの盗用などを防止することが可能な記録再生装置を提供することができる。

【0025】また、請求項2にかかる発明によれば、鍵情報を変更可能に記憶するようにしたため、各種の鍵情報を設定可能である。

【0026】さらに、請求項3にかかる発明によれば、鍵情報ROMを装着するだけで鍵情報を設定可能としたため、利用者が鍵情報を入力するなどの煩わしい操作が不要である。

【0027】さらに、請求項4にかかる発明によれば、本来のデータを記録する記録媒体に鍵情報を記録し、その鍵情報を取得して利用するようにしたため、より簡易な構成とすることができる。

【0028】さらに、請求項5にかかる発明によれば、記録媒体が脱着可能である場合に適用してより効果的に記録媒体上のデータ盗用などを防止することができる。

【0029】さらに、請求項6にかかる発明によれば、上述したセクタの論理アドレスのスクランブルに加え、データ自体にも暗号化を施すようにしたため、より効果的にデータ盗用などを防止することができ、請求項7および請求項8によれば、具体的な暗号化手法を提供することができる。

【0030】さらに、請求項9にかかる発明によれば、記録再生装置の内部に適宜インターフェイスを交換するようにしたため、汎用的なインターフェイスを有するホスト装置に適用することができ、請求項10にかかる発明によれば、具体的な適用例を提供することができる。

#### 【0031】

【発明の実施の形態】以下、図面にもとづいて本発明の実施形態を説明する。図1は、本発明の一実施形態にかかる記録再生装置を適用した光磁気ディスクドライブを斜視図により示している。同図において、光磁気ディスクドライブ10は、略矩形箱形に形成されており、筐体正面に形成された脱着孔10aを介して光磁気ディスク10bを装着可能であり、装着された光磁気ディスク10bは「EJECT」ボタン10cを押し下げるか、または本光磁気ディスクドライブ10が接続される図示しないPCから所定のコマンドを発行することにより取り出すことができる。光磁気ディスクドライブ10の筐体背面側にはSCSIコネクタケーブル10dの一端を装着可能であり、同SCSIコネクタケーブル10dの他端が上記PCのSCSIボードに装着される。

【0032】図2は、上記PCに備えられたSCSIボード20と、このSCSIボード20に接続された各種ディスクドライブとの接続形態を示している。同図において、SCSIボード20に対しては、光磁気ディスクドライブ10と、二つのSCSI仕様ハードディスクドライブ21、22とがディジーチェーン状に接続されている。ここにおいて、光磁気ディスクドライブ10に対しては1Dとして「1」を付与し、一つ目のSCSI仕様ハードディスクドライブ21については1Dとして「2」を付与し、二つ目のSCSI仕様ハードディスクドライブ22については1Dとして「3」を付与するものとする。むろん、かかる1Dを各ディスクドライブ内のSCSIコントローラが認識してアクセスをコントロールしていることはいうまでもない。

【0033】光磁気ディスクドライブ10は、概略図3に示すように構成されている。上述したように、PC側にはSCSIインターフェイスであるが、実際には光磁気ディスク10bに対してアクセスする際にはATAPIインターフェイスに変換されていることが分かる。これは本実施形態における光磁気ディスクドライブ10が汎用ATAPIデバイス11を利用してのことによる。SCSIインターフェイスとATAPIインターフェイスとは、コマンド体系において、互いにコマンドパケットでコマンドを送る点で共通し、コマンドパケットの長さにおいて相違する。すなわち、SCSIインターフェイスは6バイトのコマンドパケットを採用し、ATAPIインターフェイスは12バイトのコマンドパケットを採用している点で相違する。ただし、ATAPIインターフェイスについての後半の6バイトは将来の拡張のためにリザーブされているだけであるため、実質的には図4に示すようにダミーのコマンドを付加して長さを合わせれば良いといえる。

【0034】一方、双方のデータバスについては、パラレルでデータを送る点で共通し、バス幅において相違する。すなわち、SCSIバスは8ビット幅のバイト単位を採用し、ATAPIバスは16ビットのワード単位を採用している点で相違する。ここにおいて、転送されるデータの順序については図5に示すようにワードデータの偶数アドレスデータと奇数アドレスデータとがそれぞれバイトデータの1バイト目と2バイト目に相当している。従って、SCSIバスからATAPIバスへデータ転送するときには相連続する2バイトをそれぞれ偶数アドレスデータと奇数アドレスデータとしてワードデータに変換して転送すればよいし、ATAPIバスからSCSIバスへデータ転送するときにはワードデータの偶数アドレスデータと奇数アドレスデータとを分けて2バイトとして順次転送すればよい。

【0035】すなわち、図3を参照すると、光磁気ディスク10bにデータを記録する場合には、SCSIコントローラ12を介してSCSIバス13に入力される6

バイトのコマンドパケットをCPUで構成されるSCSIバスコントローラ14に入力し、このSCSIバスコントローラ14のコマンド変換ロジック14aによって上記のように12バイトのコマンドパケットに変換する。これとともに、SCSIバス13を介して転送されるバイトデータを図5に示す対応関係に従ってワードデータとしてセクタバッファ16に順次格納する。

【0036】周知の通り、セクタとは記録媒体に対する最小記録単位であり、本実施形態においては、図6に示すように2kバイト(2048バイト)のセクタ長を採用するものとする。従って、上記のようにしてワードデータが順次生成されてセクタバッファ16に1024個のワードデータが格納された時点で1セクタ分のデータが生成され、その後ATAPIバス15を介してセクタ単位にワードデータが転送される。一方、光磁気ディスク10bからデータを読み出す場合には上述したものと逆の手順に従って読み出せばよい。

【0037】このように異なるバス間でバス変換しつつアクセスする意義は次の事由による。近年においてはハードウェアに要求される機能を前提としてバスの仕様が求められてきているため、独自に仕様決定された異なるバスでも同じ機能に対して同じような体系が必要とならざるを得なくなってきている。従って、今日では似通った複数のバスが利用されているが、かかる場合にまで各々個別のインターフェイスを設けることは必ずしも得策ではない。そこで、上述したように適宜バス変換することにより利用上の便宜を図る。

【0038】本実施形態においては、SCSIバスとATAPIバスとの間でバス変換する構成とされているが、むしろ、実際に適用するバスとしては、今後開発されるいかなる仕様のバスについても全く同様に適用することが可能である。さらに、かかるバス変換を行うか否かは任意であり、バス変換を行わないものに対しても適用可能である。なお、バス変換についてのより詳細な構成の説明については、本願出願人による特願平9-283763号公報に開示されているため、これ以上は詳述しないこととする。

【0039】ところで、近年においては記録媒体上のデータが盗用されないように、各種のセキュリティ機能が設けられることがある。特に本実施形態においては、記録媒体として可搬性の光磁気ディスクを使用することから、光磁気ディスクが持ち出されてデータが盗用される危険性が高いと言える。そこで、本実施形態にかかる光磁気ディスクドライブ10においても、光磁気ディスク上に記録されたデータの盗用などを防止することを目的としてセキュリティ機能が備えられており、次に、このセキュリティ機能について説明する。

【0040】上述しなかったが、光磁気ディスク10bに対してデータを記録する場合に、セクタバッファ16に格納されたセクタデータ単位に後述する各種の暗号化

処理が施されて光磁気ディスク10bに記録される。むしろ、暗号化処理を施すにあたっては所定のキー情報が必要であり、本実施形態においてはかかるキー情報を記録したキーROM17として光磁気ディスクドライブ10とともに提供される。このキーROM17は、光磁気ディスクドライブ10に対して脱着可能に構成されており、光磁気ディスクドライブ10に装着した状態で、記録されたキー情報が読み取られ、キーRAM18に転送されて記憶される構成としてある。むしろ、本実施形態においては、このキーRAM18が鍵情報記憶手段を構成する。

【0041】より具体的には、図7に示すように、キーROM17をカード型に形成するとともに、光磁気ディスクドライブ10の背面側に同キーROM17を挿入可能なカード挿入孔10eを形成しておく。そして、同カード挿入孔10eにキーROM17を挿入した状態でリセットすると、リセット起動時にキーROM17に記録されたキー情報が読み出され、キーRAM18に転送されるなどの構成とすればよい。なお、本実施形態におけるキー情報としては、図8に示すように各1ビットの「ROM0」～「ROM15」のデータからなり、全体として2バイト長で構成されている。従って、キー情報のとりうる値としては65536通りとなり、仮にそれ以上の光磁気ディスクドライブ10が工場出荷された場合であっても、任意に取り出した異なる二つの光磁気ディスクドライブ10同士で同一のキー情報となる確率は極めて低いと言え、特に問題は生じない。

【0042】本実施形態においては、キー情報を提供する提供媒体としてキーROM17を採用しているが、むしろ、かかるキー情報を提供する提供媒体としてはキーROMに限られることなく適宜変更可能である。例えば、光磁気ディスク10bにデータとしてキー情報を記録しておき、このキー情報を読み取らせてキーRAM18に記憶させるようにしてもかまわない。この場合、キーROM等の専用の記録媒体を装着する機構が不要となるため、より簡易な構造にすることが可能となる。

【0043】上述したようにして1セクタ分のデータがセクタバッファ16に格納されると、まず第一にデータスクランブラ19aがデータのスクランブルを実行する。このデータスクランブラ19aは、概略図9に示すように構成されている。同図からも分かるように、データスクランブラ19aは、16個のD-FFで構成されるレジスタ19a1と、同様に16個のD-FFを巡回するように接続しつつそれぞれ別のD-FF間に16個のExOR(排他的論理和)ゲートを介在させて構成される16個のExORゲートで構成されるExORゲート群19a3とを主要回路として備えている。

【0044】レジスタ19a1を構成する各D-FFの入力端子には、それぞれキーRAM18に記憶された

「ROM0」～「ROM15」のデータが入力されるとともに、所定のクロックが入力されている。従って、レジスタはクロックパルスの立下がり毎に入力された「ROM0」～「ROM15」のキー情報をパラレルに出力することになる。

【0045】レジスタ19a1を構成する各DFFの出力は、シフトレジスタ19a2を構成する各ExORゲートに入力されるとともに、これら各ExORゲートの別の入力端子には後段側のDFFからの出力データが入力され、各ExORゲートの出力が前段側のDFFに入力されている。むしろ、シフトレジスタ19a2を構成する各DFFにも所定のクロックが入力されており、クロックの立下がり毎に各DFFからデータが出力され、前段側のExORゲートにて排他的論理和がとられて前段側のDFFに入力される。シフトレジスタ19a2は、各DFFからの出力データをスクランブル用データ「SCRD0」～「SCRD15」としてパラレルに出力しており、結果としてリセット時からカウントして16個のクロックパルスで一巡するスクランブル用データを出力していることになる。

【0046】一方、ExORゲート群19a3にはセクタバッファ16に格納されたセクタデータの各ワードデータがパラレルに順次入力されるようになっており、各ExORゲートの別の入力端子には上述したスクランブル用データ「SCRD0」～「SCRD15」がパラレルに入力されている。従って、これら各ExORゲートで排他的論理和がとられて出力されることになるが、これはワードデータが暗号化されることを意味する。このようにして、セクタバッファ16に格納されたセクタデータを構成する各ワードデータについて暗号化が終了したら、次にセクタスクランブラ19bがセクタ内におけるワードアドレスのスクランブル処理を開始する。

【0047】セクタスクランブラ19bによるワードアドレスのスクランブル処理について、説明を簡略化するため3ビットのアドレス体系として考慮する。図10は、3ビットのアドレス体系（1セクタあたり8ワード）を有するワードアドレスのスクランブル処理を行う場合において、セクタスクランブラ19bの構成の一例を概略回路図により示している。図において、x、y、zとして3ビットのアドレスをパラレルに入力し、互いに隣接する二本のアドレス伝送路に介在する複数の論理回路19b1による論理演算を経て、 $\alpha$ 、 $\beta$ 、 $\gamma$ のアドレスがパラレルに出力されるものとする。

【0048】上記の論理回路19b1は図11に示すように構成されている。ここで、入力端子A、Bおよび入力端子EXの入力パターンと、各入力パターンにおける出力端子A'、B'との対応関係は図12に示すようになる。図同からも分かるように、入力端子EXに「1」が入力される場合には、出力端子A'、B'のそれぞれから入力端子A、Bの入力データがそのまま出力される

ものと考えることができる。他方、入力端子EXに「0」が入力される場合には、出力端子A'、B'のそれぞれから入力端子A、Bの入力データが相互に入れ換えられて出力されるものと考えることができる。従って、図10に示す回路図は、概念的には図13に示すのみだくじとして考慮すればよく、論理回路19b1によって同あみだくじの枝パターンが構築されていることになる。すると、スクランブル前のワードアドレスxyzとスクランブル後のワードアドレス $\alpha\beta\gamma$ は、図14の対応表に示すようになり、スクランブル後のワードアドレスにおいてアドレス値の重複が生じないことが容易に分かる。これは、図15に示すように各ワードがセクタ内でランダムに再配置されたことを意味する。

【0049】本実施形態においては、1セクタあたり1024個のワードで構成されているため、1セクタあたり10ビットのワードアドレス（「0000h」～「3Ffh」）を考慮すればよく、複数の論理回路19b1を10ビットのアドレス伝送路に適宜配置し、各ワードアドレスをパラレルに入力してその出力をスクランブル後のワードアドレスとすればよい。なお、実際のアドレス伝送路には、合計十六個の論理回路19b1が配置されており、各論理回路19b1の入力端子EXには上述したスクランブル用データ「SCRD0」～「SCRD15」が入力されるようにしてある。上述したように、このスクランブル用データは十六種類のパターンをとりうるため、枝パターンとしても十六種類のパターンをとりうることになり、適宜枝パターンを切り換えながら実際のスクランブル処理を行う。ただし、同一のセクタにおいて枝パターンを変更すると、ワードアドレスの重複等が発生して不整合が生じるため、枝パターンの変更はセクタ単位に行うものとする。

【0050】一方、SCSIバスコントローラ14のLBAスクランブラロジック14bは、光磁気ディスク10bにおける各セクタの論理アドレスたるLBAのスクランブル処理を行い、上記のようにして変換されたコマンドパケットにおけるLBAをスクランブル後のLBAに置き換えて出力する。光磁気ディスク10bにおいては、図16に示すように各セクタは略円形の記録媒体上において円周上に順次配置されている。各セクタに対しては、それぞれを識別可能な論理アドレスが付与されており、この論理アドレスのことをLBAと言う。例えば、640メガバイト容量の光磁気ディスクの場合、LBAは「000000h」～「500000h」の範囲の値となる。

【0051】通常、記録媒体上のセクタが連続して空いている場合には、連続するセクタを跨ぐようにしてデータの記録が行われるが、LBAスクランブラロジック14bはかかる場合であっても各セクタに対するLBAにスクランブル処理を施す。例えば、図17に示すようにPC側からLBA「96h」から「3h」セクタに渡っ



てデータを記録すべくコマンド「Write (10)」が発行された場合であっても、実際に発行されるコマンドは「33h」、「23h」、「D3h」のLBAのセクタに対するコマンドに変換されて発行されることになる。

【0052】具体的には、記録媒体上のセクタとLBAとは一対一で対応しているため、上述したセクタスクランブラ19bにおけるスクランブル処理と同様に、あみだじの手法を利用してLBAをランダムに変更すればよい。むしろ、そのスクランブル処理にはキーRAM18に記憶された鍵情報を用いるが、セクタスクランブラ19bにおけるスクランブル処理のように枝パターンの変更は行わない。

【0053】一方、以上のようにしてデータ記録された光磁気ディスクからデータを読み出す場合には、逆の手順に従って復号化しつつ読み出せばよい。すなわち、LBAスクランブラロジック14bによって対象となるセクタのLBAを復元しつつ読み出してセクタバッファ16に格納し、セクタスクランブラ19bによってセクタバッファ16上でワードアドレスを復元した後、データスクランブラ19aによって各ワードを復号化して出力することになる。むしろ、これらの復号化においてはキーRAM18に記憶されたキー情報を用いられ、上述したSCSI/ATAPIのコマンド変換やバス幅変換処理等がSCSIバスコントローラ14によって行われることは言うまでもない。

【0054】ところで、LBA「00001h」～「00003h」には、通常、FAT情報が記録される。しかしながら、本実施形態においては、上述したようにLBAがスクランブル処理されるため、LBA「00001h」～「00003h」にFAT情報が記録されることは起こり得ない。とすれば、本光磁気ディスクドライブ10を用いてデータを記録した光磁気ディスク10bが持ち出されたとしても、他の再生装置ではFAT情報すら読み取ることができないため、記録されているファイルや、セクタ間のデータの関連性も判明しない。さらに、データ自体にもスクランブル処理が施されているため、光磁気ディスク10bに記録されたデータが盗用される可能性は極めて低いと言える。

【0055】このように、本実施形態においては、SCSIバスコントローラ14による制御のもとで適宜セクタバッファ16を使用してSCSI/ATAPIのバス変換を行いつつ、セクタバッファ16上でデータスクランブラ19aによってワード毎にデータを暗号化し、セクタスクランブラ19bによって同一セクタ内でワードアドレスをスクランブルするとともに、SCSIバスコントローラ14のLBAスクランブラロジック14bによってセクタのLBAをスクランブルして光磁気ディスク10bにデータを記録するようになっており、この意味においてこれらのハードウェアとソフトウェア構成と

がスクランブル記録手段を構成する。さらに、記録時と逆の手順でスクランブル解除しつつ光磁気ディスク10b上のデータを読み出すようになっている、この意味における上記のハードウェア構成とソフトウェア構成とがスクランブル解除読出手段を構成する。

【0056】次に、上記のように構成した本実施形態の動作について説明する。データ記録時において、SCSIコントローラ12を介して入力されるバイトデータは、2バイトのワードデータに変換されながら順次セクタバッファ16に格納され、全体で2kバイトとなったところで1セクタとなる。このように1セクタが生成されたら、データスクランブラ19aは予めキーRAM18に記憶されたキー情報に基づいてセクタバッファ16上で各ワード単位に暗号化する。その後に、セクタスクランブラ19bがキーRAM18に記憶されたキー情報に基づいて同一セクタ内でワードアドレスをスクランブルすることにより、各ワードを同一セクタ内でランダムに入れ換える。

【0057】一方、SCSIバスコントローラ14のコマンド変換ロジック14aは、SCSIコントローラ12を介して入力される6バイトのコマンドパケットを12バイトのコマンドパケットに変換する。これとともに、SCSIバスコントローラ14のLBAスクランブラロジック14bは、記録しようとするセクタのLBAを同様にキーRAM18に記憶されたキー情報に基づいてスクランブルするようになっている、コマンドパケットに含まれるLBAをスクランブル後のLBAに置き換えて出力する。そして、セクタバッファ16に格納されたセクタデータが出力され、汎用ATAPIデバイス11によって上記のように変換されたコマンドパケットで指定されるLBAに記録される。以降、同様にしてセクタ単位にデータ記録される。

【0058】他方、データ読出し時において、SCSIバスコントローラ14のコマンド変換ロジック14aは、SCSIコントローラ12を介して入力される6バイトのコマンドパケットを12バイトのコマンドパケットに変換する。これとともに、SCSIバスコントローラ14のLBAスクランブラロジック14bは、読み出そうとするセクタのLBAをキーRAM18に記憶されたキー情報に基づいてスクランブルしつつ、コマンドパケットに含まれるLBAをスクランブル後のLBAに置き換えて出力する。すると、汎用ATAPIデバイス11によってコマンドパケットで指定されるLBAのセクタが読み出され、セクタバッファ16に格納される。

【0059】その後、セクタスクランブラ19bはセクタバッファ16上でキーRAM18に記憶されたキー情報に基づいて同一セクタ内でスクランブルされたワードアドレスを復元することにより、各ワードを同一セクタ内で元の位置に戻す。その後に、データスクランブラ19aはセクタバッファ16上でキーRAM18に記憶さ

れたキー情報に基づいて暗号化された各ワードデータを復号化し、全てのワードデータの復号化が完了したらセクタバッファ 16 に格納されたセクタデータが SCS I コントローラ 12 を介して出力される。以降、同様にしてセクタ単位にデータが読み出される。

【0060】このように、光磁気ディスク 10 b に対してデータを記録するにあたり、データスクランブラ 19 a およびセクタスクランブラ 19 b によってデータ自体を暗号化するとともに、SCS I バスコントローラ 14 の LBA スクランブラロジック 14 b によってセクタの LBA をスクランブルしつつ記録し、記録したデータを読み出すにあたっては、SCS I バスコントローラ 14 の LBA スクランブラロジック 14 b によって LBA を復元しつつ読み出すとともに、データスクランブラ 19 a およびセクタスクランブラ 19 b によってデータ自体を復号化して出力するようにしたため、記録媒体上のセクタ間のデータの関連性がランダムとなって一般の再生装置によっては記録媒体上の F A T 情報等も読み取ることができなくなり、より確実に記録媒体上のデータの盗用などを防止することが可能な記録再生装置を提供することができる。

【図面の簡単な説明】

【図 1】本発明の一実施形態にかかる記録再生装置を適用した光磁気ディスクドライブを示す斜視図である。

【図 2】光磁気ディスクドライブの適用例を示す概略図である。

【図 3】光磁気ディスクドライブの構成を示す概略ブロック図である。

【図 4】SCS I バスと A T A P I バスのコマンドバケットを示す図である。

【図 5】SCS I バスと A T A P I バスにおけるバイトデータとワードデータの対応関係を示す図である。

【図 6】1024 個のワードによって 1 セクタが構成されることを示す図である。

【図 7】光磁気ディスクドライブにキー ROM を装着する過程を示す斜視図である。

\* 【図 8】キー ROM に記録されたキー情報を概念的に示す図である。

【図 9】データスクランブラの主要構成回路を示す概略回路図である。

【図 10】セクタスクランブラの主要構成回路を説明するための概略回路図である。

【図 11】同セクタスクランブラに備えられた論理回路の構成を示す図である。

【図 12】同論理回路の入力パターンと出力パターンの対応関係を示す図である。

【図 13】セクタスクランブラによる処理を概念的に示す図である。

【図 14】3 ビットのワードアドレスがスクランブルされたことを示す図である。

【図 15】セクタ内でワードがランダムに再配置されることを概念的に示す図である。

【図 16】光磁気ディスク上のセクタと LBA の関係を示す図である。

【図 17】LBA がスクランブルされたコマンド例を示す図である。

【符号の説明】

10…光磁気ディスクドライブ

11…汎用 A T A P I デバイス

12…SCS I コントローラ

13…SCS I バス

14…SCS I バスコントローラ

14 a…コマンド変換ロジック

14 b…LBA スクランブラロジック

15…A T A P I バス

16…セクタバッファ

17…キー ROM

18…キー RAM

19 a…データスクランブラ

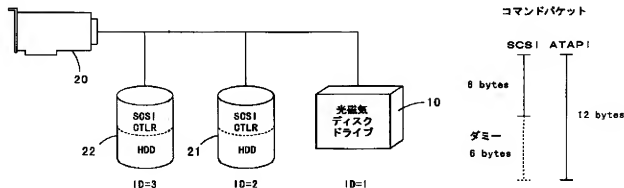
19 b…セクタスクランブラ

19 b 1…論理回路

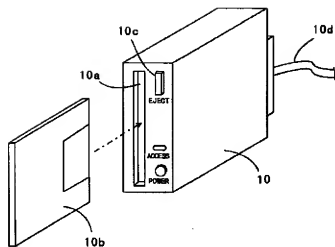
20…SCS I ボード

【図 2】

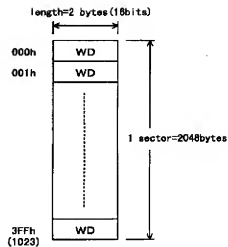
【図 4】



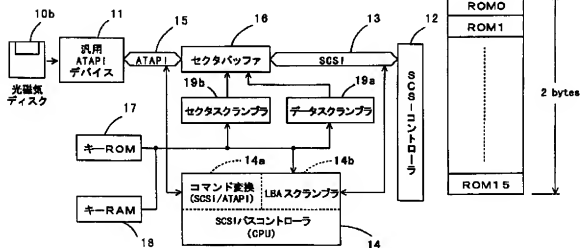
【図1】



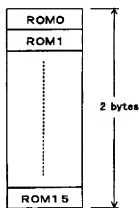
【図6】



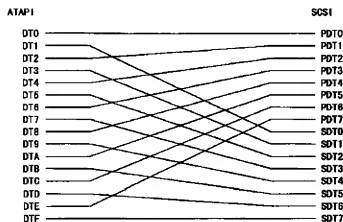
【図3】



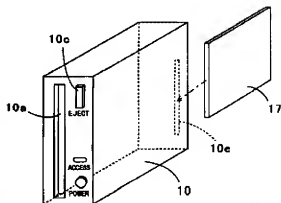
【図8】



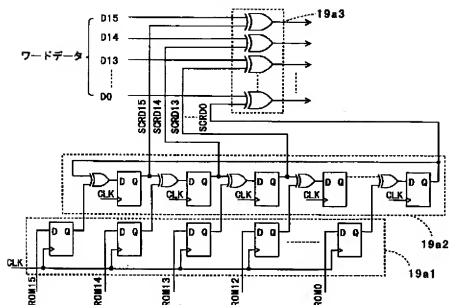
【図5】



【図7】



【図9】

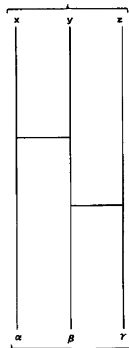


【図12】

		EX=1		EX=0	
		A	B	A'	B'
0	0	0	0	0	0
1	0	1	0	0	1
0	1	0	1	1	0
1	1	1	1	1	1

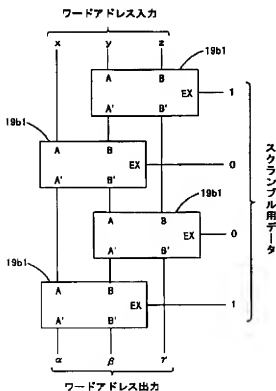
【図13】

ワードアドレス入力

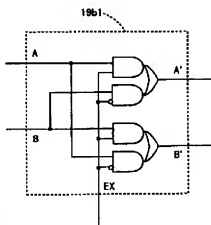


ワードアドレス出力

【図10】



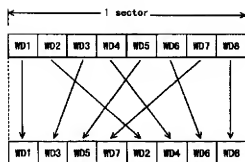
【図11】



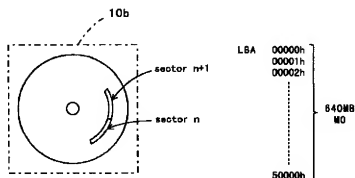
【図14】

スクランブル前 x y z	スクランブル後 α β γ
000	000
001	010
010	100
011	110
100	001
101	011
110	101
111	111

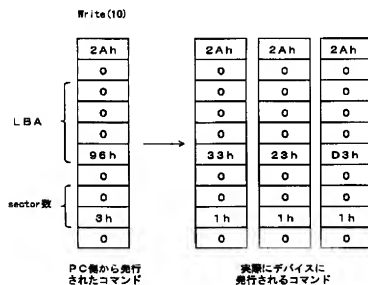
【図15】



【図16】



【図17】



フロントページの続き

F ターム(参考) 5B017 AA07 BA07 BB03 CA07 CA09  
 5D044 BCD1 BC06 CC04 DE03 DE12  
 DE38 EF03 FG10 GK17 GL02  
 GL18 HL11